AMENDMENTS TO THE CLAIMS

1. (CURRENTLY AMENDED) A method in a unified communications system, the method comprising:

receiving from a requesting device a request for providing a user interface session by the unified communications system to enable a user of the requesting device to send a message to an identified destination subscriber;

receiving, by the unified communications system, the message in unencrypted form from the requesting device as part of the user interface session;

generating [[for]] and outputting to the requesting device as part of the user interface session a first prompt enabling the user to select encryption of the message;

generating [[for]] and outputting to the requesting device as part of the user interface session a second prompt, based on the user selecting encryption of the message, for the user to input an encryption key;

invoking a resource configured for executing encryption of the message, having been received in unencrypted form, into an encrypted message based on the encryption key received from the requesting device as part of the user interface session, the resource and the executing encryption being distinct from the requesting device; and

outputting the encrypted message to a determined destination based on determined subscriber profile attributes for the identified destination subscriber.

2. (CANCELED).

3. (CURRENTLY AMENDED) The method of claim 1, wherein the ~~step of~~ receiving of the message includes receiving a message data file having the message and a Multipurpose Internet Mail Extension (MIME) that specifies a format of the message, the invoking ~~step~~ including encrypting the message data file into an encrypted file having a MIME extension specifying that the encrypted file has an encrypted format.

4. (PREVIOUSLY PRESENTED) The method of claim 3, further including generating a message transport header specifying an IP based destination address corresponding to the identified destination subscriber.

5. (CURRENTLY AMENDED) The method of claim 3, wherein the message data file has a MIME extension specifying a ".wav" format, the message having an audio header and audio payload, the invoking [[step]] including encrypting the audio header and the audio payload within the encrypted file.

6. (ORIGINAL) The method of claim 1, further comprising determining the subscriber profile attributes for the identified destination subscriber based on accessing a subscriber directory according to Lightweight Directory Access Protocol (LDAP), the subscriber profile attributes specifying the determined destination.

7. (CURRENTLY AMENDED) The method of claim 1, wherein the outputting [[step]] includes outputting the encrypted message to the determined destination according to at least one of SMTP protocol and IMAP protocol.

8. (CURRENTLY AMENDED) The method of claim 1, further comprising:

receiving from a second requesting device a request for providing a second user interface session by the unified communications system to enable the identified destination subscriber using the second requesting device to retrieve stored messages;

retrieving for the second user interface session information related to the stored messages for the identified destination subscriber;

detecting one of the stored messages as encrypted;

generating for the second requesting device as part of the second user interface session a third prompt, based on detecting the one stored message, for the identified destination subscriber to input a decryption key; and

supplying the decryption key having been received from the second requesting device as part of the second user interface session and the one stored message to an invoked decryption utility for decryption of the one stored message into a decrypted data file, the invoked decryption utility and the decryption distinct from the requesting device and the second requesting device.

9. (PREVIOUSLY PRESENTED) The method of claim 8, further comprising outputting a decryption result, having been received from the invoked decryption utility relative to the supplying of the decryption key and one stored message, during the second user interface session to the identified destination subscriber, independent of the encryption key matching the decryption key.

10. (CURRENTLY AMENDED) The method of claim 1, wherein the receiving [[step]] of the request includes receiving the request according to hypertext transport protocol, each of the ~~steps of~~ generating the first prompt and generating the second prompt including sending a corresponding HTML page specifying the corresponding prompt, the ~~step of~~ receiving of the message includes receiving the message as an HTTP post to a prescribed uniform resource location.

11. (CURRENTLY AMENDED) A method in a unified communications system, the method comprising:

receiving from a requesting device a request for providing a user interface session by the unified communications system to enable a messaging subscriber using the requesting device to retrieve stored messages;

accessing, for the user interface session, subscriber profile information from a subscriber profile directory according to a prescribed open network protocol, the subscriber profile directory distinct from the requesting device;

determining one of the stored messages is encrypted based on access of a message store according to a prescribed open network protocol and based on the accessed subscriber profile information;

generating [[for]] and outputting to the requesting device as part of the user interface session a prompt, based on identifying the one stored message as encrypted, for the messaging subscriber to input a decryption key; and

invoking a resource configured for attempting decrypting of the one stored message based on the decryption key having been supplied by the messaging subscriber via the requesting device as part of the user interface session, the resource and the attempting decrypting being distinct from the requesting device.

12. (CURRENTLY AMENDED) The method of claim 11, further comprising:

obtaining a decryption result based on the invoking ~~step~~ of the resource; and

outputting the decryption result for attempted presentation to the messaging subscriber.

13. (ORIGINAL) The method of claim 12, wherein the outputting step includes outputting the decryption result independent of whether the decryption key enabled successful decryption of the one stored message.

14. (CANCELED).

15. (CURRENTLY AMENDED) The method of claim 11, further comprising obtaining, based on the invoking ~~step~~ of the resource, a decryption result including a message data file having a message and a Multipurpose Internet Mail Extension (MIME) that specifies a format of the message.

16. (CURRENTLY AMENDED) The method of claim 11, wherein the receiving ~~step~~ of the request includes receiving the request according to hypertext transport protocol, wherein the ~~step of~~ generating of the prompt includes outputting a first HTML page specifying the prompt.

17. (CURRENTLY AMENDED) The method of claim 11, wherein the accessing ~~step~~ includes obtaining the subscriber profile information according to LDAP protocol.

18. (CURRENTLY AMENDED) The method of claim 17, wherein the determining [[step]] includes:

accessing the message store according to IMAP protocol for messaging information related to the stored messages for the messaging subscriber, based on the accessed subscriber profile information; and

identifying the one stored message as encrypted based on a prescribed file extension specifying that the one stored message has an encrypted format.

19. (CURRENTLY AMENDED) The method of claim 18, wherein the identifying [[step]] includes identifying the prescribed file extension as a MIME type extension that specifies an encrypted format.

20. (CURRENTLY AMENDED) The method of claim 11, wherein the determining [[step]] includes:

accessing the message store according to IMAP protocol for messaging information related to the stored messages for the messaging subscriber, based on the accessed subscriber profile information; and

identifying the one stored message as encrypted based on a prescribed file extension specifying that the one stored message has an encrypted format.

21. (CURRENTLY AMENDED) The method of claim 20, wherein the identifying [[step]] includes identifying the prescribed file extension as a MIME type extension that specifies an encrypted format.

22. (CURRENTLY AMENDED) A unified communications server including:

an interface configured for receiving a request from a requesting device for generation of a user interface session by the unified communications server to enable a user of the requesting device to send a message to an identified destination subscriber;

an IP-based interface enabling retrieval of subscriber profile attributes for the identified destination subscriber from an IP-based subscriber profile directory that is distinct from the requesting device, and storage of messaging information for the identified destination subscriber in an IP-based subscriber message store that is distinct from the requesting device; and

an application runtime environment configured for generating the user interface session and accessing the subscriber profile attributes, the application runtime environment configured for generating first and second prompts [[for]] and outputting the first and second prompts to the requesting device as part of the user interface session enabling the user to select encryption of the message and input an encryption key, respectively, the application runtime environment configured for invoking a resource configured for encrypting the message, received in unencrypted form from the requesting device as part of the user interface session, into an encrypted file based on the encryption key supplied by the user via the requesting device as part of the user interface session, and outputting an encrypted message including the encrypted file for storage in the IP-based subscriber message store for the identified destination subscriber, the resource and the encrypting distinct from the requesting device.

23. (CANCELED).

24. (PREVIOUSLY PRESENTED) The server of claim 22, wherein the application runtime environment is configured for generating for the encrypted message a MIME extension

specifying that the encrypted file has an encrypted format, and a message transport header specifying an IP based destination address corresponding to the identified destination subscriber.

25. (PREVIOUSLY PRESENTED) The server of claim 22, wherein the IP-based interface includes an application programming interface configured for invoking prescribed routines, including a first routine for accessing the IP-based subscriber profile directory according to LDAP protocol, and a second routine for accessing the IP-based subscriber message store according to at least one of SMTP protocol and IMAP protocol.

26. (PREVIOUSLY PRESENTED) The server of claim 25, wherein the application programming interface is configured for implementing the invoking of the resource by the application runtime environment for generation of the encrypted message.

27. (CURRENTLY AMENDED) The server of claim 22, wherein the application runtime environment is further configured for generating a second user interface session for a second requesting device enabling the identified destination subscriber using the second requesting device to retrieve stored messages, the application runtime environment, in response to detecting one of the stored messages as encrypted, generating a third prompt for the second requesting device as part of the second user interface session to enable the identified destination subscriber to input a decryption key, the application runtime environment configured for invoking a second resource configured for attempting decryption of the one stored message based on the decryption key input by the user via the second requesting device as part of the user interface session, the second resource distinct from the requesting device and the second requesting device.

28. (ORIGINAL) The server of claim 27, wherein the application runtime environment, upon obtaining a decryption result based on the attempted decryption, outputs the decryption

result for attempted presentation to the identified destination subscriber independent of whether the decryption key enabled successful decryption of the one stored message.

29. (ORIGINAL) The server of claim 22, wherein the interface is configured for receiving the request, and outputting responses, according to hypertext transport protocol.

30. (CURRENTLY AMENDED) A unified communications server comprising:

an interface configured for receiving from a requesting device a request for generation of a user interface session by the unified communications server to enable a messaging subscriber using the requesting device to retrieve stored messages;

an IP-based interface enabling retrieval of subscriber profile attributes for the messaging subscriber from an IP-based subscriber profile directory that is distinct from the requesting device, and access of messaging information for the messaging subscriber from an IP-based subscriber message store that is distinct from the requesting device; and

an application runtime environment configured for generating the user interface session and accessing the subscriber profile attributes, the application runtime environment configured for generating, based on identifying from the messaging information that one of the stored messages is encrypted, a prompt [[for]] output to the requesting device as part of the user interface session enabling the messaging subscriber to input a decryption key, the application runtime environment configured for invoking a resource configured for attempting decryption of the one stored message into a decryption result based on the decryption key supplied by the user via the requesting device as part of the user interface session, the resource and the attempting decryption being distinct from the requesting device.

31. (CANCELED).

32. (PREVIOUSLY PRESENTED) The server of claim 30, wherein the application runtime environment is configured for outputting the decryption result to the messaging

subscriber independent of whether the decryption key enabled successful decryption of the one stored message.

33. (ORIGINAL) The server of claim 30, wherein the application runtime environment identifies that the one stored message is encrypted based on an attached MIME extension specifying an encrypted format.

34. (PREVIOUSLY PRESENTED) The server of claim 30, wherein the IP-based interface includes an application programming interface configured for invoking prescribed routines, including a first routine for accessing the IP-based subscriber profile directory according to LDAP protocol, and a second routine for accessing the IP-based subscriber message store according to IMAP protocol.

35. (PREVIOUSLY PRESENTED) The server of claim 34, wherein the application programming interface is configured for implementing the invoking of the resource by the application runtime environment for generation of the decryption result.

36. (PREVIOUSLY PRESENTED) The server of claim 30, wherein the interface is configured for receiving the request, and outputting responses, according to hypertext transport protocol.

37. (CURRENTLY AMENDED) A computer readable medium having stored thereon sequences of instructions for a device receiving a message for an identified messaging subscriber, the sequences of instructions including instructions for performing the steps of:

receiving from a requesting device a request for providing a user interface session by the device executing the instructions to enable a user of the requesting device to send a message to an identified destination subscriber;

receiving the message in unencrypted form from the requesting device as part of the user interface session;

generating [[for]] and outputting to the requesting device as part of the user interface session a first prompt enabling the user to select encryption of the message;

generating [[for]] and outputting to the requesting device as part of the user interface session a second prompt, based on the user selecting encryption of the message, for the user to input an encryption key;

invoking a resource configured for executing encryption of the message, having been received in unencrypted form, into an encrypted message based on the encryption key received from the requesting device as part of the user interface, the resource and the executing encryption being distinct from the requesting device; and

outputting the encrypted message to a determined destination based on determined subscriber profile attributes for the identified destination subscriber.

38. (CANCELED).

39. (PREVIOUSLY PRESENTED) The medium of claim 37, wherein the step of receiving the message includes receiving a message data file having the message and a Multipurpose Internet Mail Extension (MIME) that specifies a format of the message, the invoking step including encrypting the message data file into an encrypted file having a MIME extension specifying that the encrypted file has an encrypted format.

40. (PREVIOUSLY PRESENTED) The medium of claim 39, wherein the invoking step further including generating a message transport header specifying an IP based destination address corresponding to the identified destination subscriber.

41. (PREVIOUSLY PRESENTED) The medium of claim 39, wherein the message data file has a MIME extension specifying a ".wav" format, the message having an audio header and

audio payload, the invoking step including encrypting the audio header and the audio payload within the encrypted file.

42. (ORIGINAL) The medium of claim 37, further comprising instructions for performing the step of determining the subscriber profile attributes for the identified destination subscriber based on accessing a subscriber directory according to Lightweight Directory Access Protocol (LDAP), the subscriber profile attributes specifying the determined destination.

43. (ORIGINAL) The medium of claim 37, wherein the outputting step includes outputting the encrypted message to the determined destination according to at least one of SMTP protocol and IMAP protocol.

44. (CURRENTLY AMENDED) The medium of claim 37, further comprising instructions for performing the steps of:

receiving from a second requesting device a request for providing a second user interface session by the device to enable the identified destination subscriber using the second requesting device to retrieve stored messages;

retrieving for the second user interface session information related to the stored messages for the identified destination subscriber;

detecting one of the stored messages as encrypted;

generating for the second requesting device as part of the second user interface session a third prompt, based on detecting the one stored message, for the identified destination subscriber to input a decryption key; and

supplying the decryption key having been received from the second requesting device as part of the second user interface session and the one stored message to an invoked decryption utility for decryption of the one stored message into a decrypted data file, the invoked decryption utility and the decryption distinct from the requesting device and the second requesting device.

45. (PREVIOUSLY PRESENTED) The medium of claim 44, further comprising instructions for performing the step of outputting a decryption result, having been received from the invoked decryption utility relative to the supplying of the decryption key and one stored message, during the second user interface session to the identified destination subscriber, independent of the encryption key matching the decryption key.

46. (PREVIOUSLY PRESENTED) The medium of claim 37, wherein the receiving step includes receiving the request according to hypertext transport protocol, each of the steps of generating the first prompt and generating the second prompt including sending a corresponding HTML page specifying the corresponding prompt, the step of receiving the message includes receiving the message as an HTTP post to a prescribed uniform resource location.

47. (CURRENTLY AMENDED) A computer readable medium having stored thereon sequences of instructions for a device retrieving a message for a messaging subscriber, the sequences of instructions including instructions for performing the steps of:

receiving from a requesting device a request for providing a user interface session by the device executing the instructions to enable a messaging subscriber using the requesting device to retrieve stored messages;

accessing, for the user interface session, subscriber profile information from a subscriber profile directory according to a prescribed open network protocol, the subscriber profile directory distinct from the requesting device;

determining one of the stored messages is encrypted based on access of a message store according to a prescribed open network protocol and based on the accessed subscriber profile information;

generating [[for]] and outputting to the requesting device as part of the user interface session a prompt, based on identifying the one stored message as encrypted, for the messaging subscriber to input a decryption key; and

invoking a resource configured for attempting decrypting of the one stored message based on the decryption key having been supplied by the messaging subscriber via the requesting device as part of the user interface session, the resource and the attempting decrypting being distinct from the requesting device.

48. (PREVIOUSLY PRESENTED) The medium of claim 47, further comprising instructions for performing the steps of:

obtaining a decryption result based on the invoking step; and

outputting the decryption result for attempted presentation to the messaging subscriber.

49. (ORIGINAL) The medium of claim 48, wherein the outputting step includes outputting the decryption result independent of whether the decryption key enabled successful decryption of the one stored message.

50. (CANCELED).

51. (PREVIOUSLY PRESENTED) The medium of claim 47, further comprising instructions for performing the step of obtaining, based on the invoking step, a decryption result including a message data file having a message and a Multipurpose Internet Mail Extension (MIME) that specifies a format of the message.

52. (PREVIOUSLY PRESENTED) The medium of claim 47, wherein the receiving step includes receiving the request according to hypertext transport protocol, wherein the step of generating the prompt includes outputting a first HTML page specifying the prompt.

53. (ORIGINAL) The medium of claim 47, wherein the accessing step includes obtaining the subscriber profile information according to LDAP protocol.

54. (ORIGINAL) The medium of claim 53, wherein the determining step includes:

accessing the message store according to IMAP protocol for messaging information related to the stored messages for the messaging subscriber, based on the accessed subscriber profile information; and

identifying the one stored message as encrypted based on a prescribed file extension specifying that the one stored message has an encrypted format.

55. (ORIGINAL) The medium of claim 54, wherein the identifying step includes identifying the prescribed file extension as a MIME type extension that specifies an encrypted format.

56. (ORIGINAL) The medium of claim 47, wherein the determining step includes:

accessing the message store according to IMAP protocol for messaging information related to the stored messages for the messaging subscriber, based on the accessed subscriber profile information; and

identifying the one stored message as encrypted based on a prescribed file extension specifying that the one stored message has an encrypted format.

57. (ORIGINAL) The medium of claim 56, wherein the identifying step includes identifying the prescribed file extension as a MIME type extension that specifies an encrypted format.

58. (CURRENTLY AMENDED) A unified communications system comprising:

means for receiving from a requesting device a request for providing a user interface session by the system to enable a user of the requesting device to send a message to an identified destination subscriber, the means for receiving configured for receiving the message in unencrypted form from the requesting device as part of the user interface session;

means for generating [[for]] and outputting to the requesting device as part of the user interface session a first prompt enabling the user to select encryption of the message;

means for generating [[for]] and outputting to the requesting device as part of the user interface session a second prompt, based on the user selecting encryption of the message, for the user to input an encryption key;

means for invoking a resource configured for executing encryption of the message, having been received in unencrypted form, into an encrypted message based on the encryption key received from the requesting device as part of the user interface session, the resource and the executing encryption distinct from the requesting device; and

means for outputting the encrypted message to a determined destination based on determined subscriber profile attributes for the identified destination subscriber.

59. (CANCELED).

60. (PREVIOUSLY PRESENTED) The system of claim 58, wherein the means for receiving is configured for receiving the message within a message data file having the message and a Multipurpose Internet Mail Extension (MIME) that specifies a format of the message, the means for invoking configured for causing encryption of the message data file into an encrypted file having a MIME extension specifying that the encrypted file has an encrypted format.

61. (PREVIOUSLY PRESENTED) The system of claim 60, wherein the means for invoking is configured for generating a message transport header specifying an IP based destination address corresponding to the identified destination subscriber.

62. (PREVIOUSLY PRESENTED) The system of claim 60, wherein the message data file has a MIME extension specifying a ".wav" format, the message having an audio header and audio payload, the means for invoking causing the audio header and the audio payload to be encrypted within the encrypted file.

63. (ORIGINAL) The system of claim 58, further comprising means for determining the subscriber profile attributes for the identified destination subscriber based on accessing a subscriber directory according to Lightweight Directory Access Protocol (LDAP), the subscriber profile attributes specifying the determined destination.

64. (ORIGINAL) The system of claim 58, wherein the outputting means is configured for outputting the encrypted message to the determined destination according to at least one of SMTP protocol and IMAP protocol.

65. (CURRENTLY AMENDED) The system of claim 58, wherein the receiving means also is configured for receiving a request from a second requesting device for providing a second user interface session by the system to enable the identified destination subscriber using the second requesting device to retrieve stored messages, the system further comprising:

means for retrieving for the second user interface session information related to the stored messages for the identified destination subscriber;

means for detecting one of the stored messages as encrypted;

means for generating for the second requesting device as part of the second user interface session a third prompt, based on detecting the one stored message, for the identified destination subscriber to input a decryption key; and

means for supplying the decryption key having been received from the second requesting device as part of the second user interface session and the one stored message to an invoked decryption utility for decryption of the one stored message into a decrypted data file, the invoked decryption utility and the decryption distinct from the requesting device and the second requesting device.

66. (PREVIOUSLY PRESENTED) The system of claim 65, further comprising means for outputting a decryption result, having been received from the invoked decryption utility relative to the supplying of the decryption key and one stored message, during the second user

interface session to the identified destination subscriber, independent of the encryption key matching the decryption key.

67. (PREVIOUSLY PRESENTED) The system of claim 58, wherein the receiving means is configured for receiving the request according to hypertext transport protocol, wherein the first prompt is output in an HTML page to the requesting device, the second prompt output to in a second HTML page to the requesting device, the message received as an HTTP post to a prescribed uniform resource location.

68. (CURRENTLY AMENDED) A unified communications system comprising:

means for receiving from a requesting device a request for providing a user interface session by the system to enable a messaging subscriber using the requesting device to retrieve stored messages;

means for accessing, for the user interface session, subscriber profile information from a subscriber profile directory according to a prescribed open network protocol, the subscriber profile directory distinct from the requesting device;

means for determining one of the stored messages is encrypted based on access of a message store according to a prescribed open network protocol and based on the accessed subscriber profile information;

means for generating [[for]] and outputting to the requesting device as part of the user interface session a prompt, based on identifying the one stored message as encrypted, for the messaging subscriber to input a decryption key; and

means for invoking a resource configured for attempting decrypting of the one stored message based on the decryption key having been supplied by the messaging subscriber via the requesting device as part of the user interface session, the resource and the attempting decrypting being distinct from the requesting device.

69. (PREVIOUSLY PRESENTED) The system of claim 68, further comprising:

means for obtaining a decryption result based on the invoking of the resource; and

means for outputting the decryption result for attempted presentation to the messaging subscriber.

70. (ORIGINAL) The system of claim 69, wherein the outputting means is configured for outputting the decryption result independent of whether the decryption key enabled successful decryption of the one stored message.

71. (CANCELED).

72. (PREVIOUSLY PRESENTED) The system of claim 68, wherein the means for invoking obtains a decryption result including a message data file having a message and a Multipurpose Internet Mail Extension (MIME) that specifies a format of the message.

73. (PREVIOUSLY PRESENTED) The system of claim 68, wherein the receiving means is configured for receiving the request according to hypertext transport protocol, wherein the prompt is output in an HTML page to the requesting device.

74. (ORIGINAL) The system of claim 68, wherein the accessing means is configured for obtaining the subscriber profile information according to LDAP protocol.

75. (ORIGINAL) The system of claim 74, wherein the determining means is configured for:

accessing the message store according to IMAP protocol for messaging information related to the stored messages for the messaging subscriber, based on the accessed subscriber profile information; and

identifying the one stored message as encrypted based on a prescribed file extension specifying that the one stored message has an encrypted format.

76. (ORIGINAL) The system of claim 75, wherein the determining means identifies the prescribed file extension as a MIME type extension that specifies an encrypted format.

77. (ORIGINAL) The system of claim 68, wherein the determining means is configured for:

accessing the message store according to IMAP protocol for messaging information related to the stored messages for the messaging subscriber, based on the accessed subscriber profile information; and

identifying the one stored message as encrypted based on a prescribed file extension specifying that the one stored message has an encrypted format.

78. (ORIGINAL) The system of claim 77, wherein the determining means is configured for identifying the prescribed file extension as a MIME type extension that specifies an encrypted format.